Password Policy

Last Updated Friday, 02 January 2009

Overview Passwords are an important aspect of computer security for the City. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of City of Frankfort's entire corporate network. As such, all City of Frankfort employees (including contractors and vendors with access to City of Frankfort systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.
Purpose The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.
Scope The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any City facility, has access to the City network, or stores any non-public City of Frankfort information.
General Policy
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- User accounts that have special privileges granted through group memberships or programs such as remote access must have a unique password from all other accounts held by that user.
- All system-level passwords (e.g., root, enable, admin, administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.
- (Note: This applies to IT Staff only) Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below. General Password Construction Guidelines:

Passwords are used for various purposes at City of Frankfort. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router or firewall logins. Everyone should be aware of how to select strong passwords.

Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is creating a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
NOTE: Do not use either of these examples as passwords! Create a strong password that:
- contains both upper and lower case characters (e.g., a-z, A-Z)
- has digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~=\`{}[]:";'<>?,./)
- is at least eight alphanumeric characters.
- is NOT a word in any language, slang, dialect, jargon, etc.
- is NOT based on personal information, names of family, etc. Don't create a weak password that:
- contains less than 8 characters.
- is a word found in a dictionary (English or foreign language)

- is a common usage word such as:
- Names of family, pets, friends, co-workers, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, QWERTY, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)Additional lists of "dos" and "don'ts":

Don't reveal a password over the phone to ANYONE.
Don't reveal a password in an email message.
Don't reveal a password to anyone.
Don't talk about a password in front of others.
Don't hint at the format of a password (e.g., "my family name")
Don't reveal a password on questionnaires or security forms.
Don't share a password with family members.
Don't reveal a password to co-workers while on vacation.

If someone demands a password, refer them to this document or have them call someone in the IT Department.

Do not use the "Remember Password" feature of applications (e.g., OutLook, Firefox)

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Blackberry, Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to IT Department and change all passwords immediately or as soon as possible.

Password cracking or guessing may be performed on a periodic or random basis by IT Department. If a password is guessed or cracked during one of these scans, the user will be required to change it.

As an example: A six-letter password can be broken within a couple of minutes by automated password cracking programs that hackers can download from the Internet. It takes a year to crack a password containing at least eight letters, with both upper and lower case. Substitute a number for one of the letters and it would take 800 thousand years to crack.Password Protection Standards:

Do not use the same password for City of Frankfort accounts as for other non-City of Frankfort access (e.g., personal ISP account, banks, online membership, etc.). Wherever possible, don't use the same password for various City of Frankfort access needs. For example, select one password for e-mail system and a separate password for server login. Also, select a separate password to be used for a financial system account and a personnel system account.
Do not share City of Frankfort passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential City of Frankfort information. Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, based on the City Policy as stated in the Employee Handbook.

Note: To ease the burden of learning the new technology deployed in the City, the IT Department will schedule and conduct a "Lunch and Learn session" at City of Frankfort Technology Center regularly to teach every employee about computer and Internet security, electronic email, office productivity software, etc. Stay tuned and what's out for an online sign up sheet in the City's Outlook calendar.

-JP

Adapted from The SANS (SysAdmin, Audit, Network, Security) Institute.